

AD-A142 835

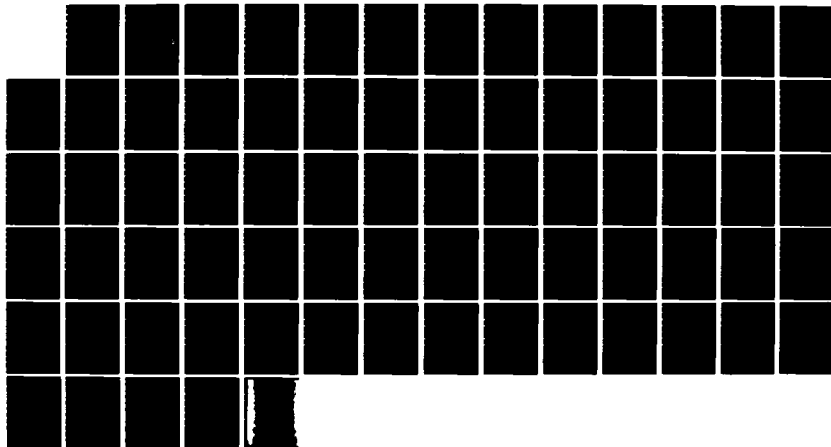
COMPUTER AND DATA SECURITY IN HOSPITALS(U) AIR FORCE
INST OF TECH WRIGHT-PATTERSON AFB OH R D WRIGHT
12 MAY 84 AFIT/CI/NR-84-26T

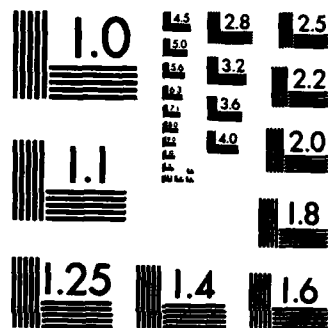
1/1

UNCLASSIFIED

F/G 9/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFIT/CI/NR 84-26T	2. GOVT ACCESSION NO. AD-A142 835	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Computer and Data Security in Hospitals	5. TYPE OF REPORT & PERIOD COVERED THESIS/DISSERTATION	
	6. PERFORMING ORG. REPORT NUMBER	
7. AUTHOR(s) Raymond D. Wright	8. CONTRACT OR GRANT NUMBER(s)	
9. PERFORMING ORGANIZATION NAME AND ADDRESS AFIT STUDENT AT: Trinity University	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS	
11. CONTROLLING OFFICE NAME AND ADDRESS AFIT/NR WPAFB OH 45433	12. REPORT DATE 1984	
	13. NUMBER OF PAGES 63	
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCLASS	
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE	
16. DISTRIBUTION STATEMENT (of this Report) APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report) A		
18. SUPPLEMENTARY NOTES APPROVED FOR PUBLIC RELEASE: IAW AFR 190-1 Lynn E. Wolaver 3/24/84 Dean for Research and Professional Development AFIT, Wright-Patterson AFB OH		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) ATTACHED		

84 07 10 159

DD FORM 1 JAN 73 1473

EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

DTIC FILE COPY AD-A142 835

Computer and Data Security in Hospitals

By

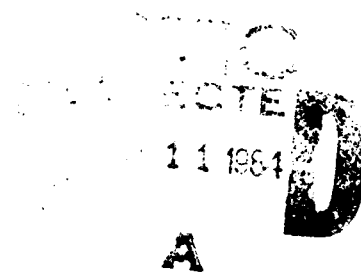
Raymond D. Wright, Capt, USAF, MSC

1984

63 Pages

Master of Science in Computer Science

Trinity University



Computer and Data Security in Hospitals

ABSTRACT OF THESIS

Presented to the Faculty of Trinity University
in Partial Fulfillment of the Requirements

For the Degree of
Master of Science

By

Raymond D. Wright, B.A.

Recent news stories in both the printed and electronic media have shown the simplicity of bypassing computer security controls and gaining access to the sensitive data stored in the computer. The most recent example is the penetration of the computers at both the Los Alamos Research Center and the Sloan-Kettering Medical Institute by a group of teenagers. From the individuals' point of view, penetration of the Sloan-Kettering Medical Institute's computer was the more serious, because the institute treats patients, teaches and trains physicians, and conducts extensive medical research. Not only was valuable research data compromised but also sensitive personal information--the individuals' confidential medical information.

This thesis will investigate and describe various methods used to protect the hospital's data and the equipment which stores, retrieves,

→ and processes it. Based upon this investigation, the most optimal method or methods of data and equipment protection will be recommended.

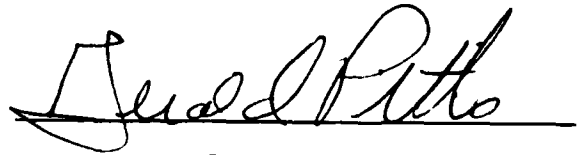


Accession For	
NO	1
	<input checked="checked" type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
S	
A-1	

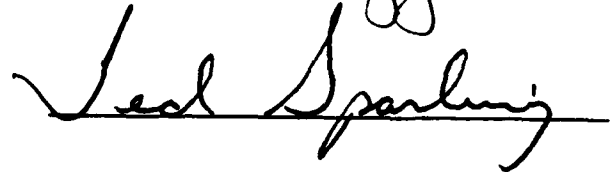
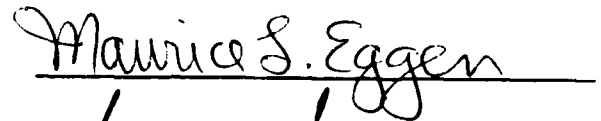
Computer and Data Security in Hospitals

Raymond D. Wright

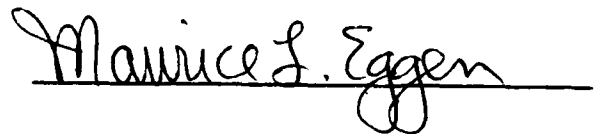
APPROVED BY THE THESIS COMMITTEE:



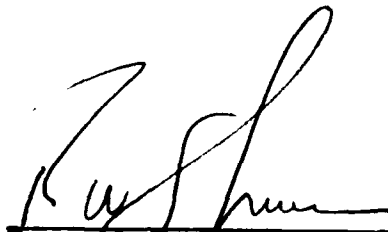
Chairperson



APPROVED BY THE CHAIRPERSON OF THE DEPARTMENT:



APPROVED BY THE DEAN:



Dean of the Division of
Business and Administrative Studies

May 12, 1984

Computer and Data Security in Hospitals

By

RAYMOND D. WRIGHT, B.A.

THESIS

Presented to the Faculty of Trinity University

in Partial Fulfillment of the Requirements

For the Degree of

Master of Science

TRINITY UNIVERSITY

May 1984

TABLE OF CONTENTS

Chapter

I.	INTRODUCTION	1
II.	THE HOSPITAL INFORMATION SYSTEM	10
III.	THE NEED TO PROTECT COMPUTERS AND DATA	20
IV.	THE METHODS OF PROTECTION	30
V.	DEFICIENCIES IN HOSPITAL INFORMATION SYSTEMS	44
VI.	CONCLUSION AND RECOMMENDATIONS	55
	BIBLIOGRAPHY	61

ILLUSTRATIONS

Figure

- 4.1 COMPUTER CENTER FLOOR PLAN. 35
- 4.2 PARTIAL DIAGRAM OF AN ELECTRONIC LOCK 35

CHAPTER I

INTRODUCTION

In the analysis of information systems, it must be understood that the terms "Data" and "Information" have separate and distinct meanings. Even though these terms are used interchangeably, it is important for the reader to understand this difference; Data are raw facts. Information is processed data. An example will further clarify this difference. If one has a name, a social security number and an address, one has three facts (data), which by themselves mean nothing. However, if one combines (processes) these facts (data), one now has information.

The main advantage for using a computer is its ability to process data very quickly and very accurately. This capability, along with improved program development methods and lower costs for obtaining and operating a computer system, has led to the wide spread use of computers in our society.¹

We live in the computer age. Our society is being molded by this machine. We are entering the age of high technology and the changes, which our society is undergoing, are immense. Yet, this age began very innocuously.

The first computers were used for scientific research and by the

¹Chris Mader, Information Systems: Technology, Economics, Applications (Chicago: Science Research Associates, Inc., 1974), p. 7.

government, mainly for military applications.² The digital computer age began in 1944, when the Harvard Mark I became operational. In 1946 ENIAC (Electronic Numerical Integrator and Calculator) was completed. This computer was produced for the U.S. Army Ordnance Department to calculate ballistic tables.³ The EDVAC (Electronic Discrete Variable Computer) was completed in 1951 and was used by Princeton University for scientific research; it became the prototype for the various computers developed at other universities. Also, the UNIVAC I (Universal Automatic Computer) was completed in 1951 and was used by the Census Bureau. In 1954 the UNIVAC I became the first computer to be used for commercial purposes. The UNIVAC I was first used by the General Electric Park in Louisville, Kentucky.⁴

In the years that followed, most businesses and government agencies have acquired computers. With the advancement in computer technology, more manual jobs were automated. As government and businesses began to automate their personnel files, people became concerned about the use of this information and the measures implemented to protect the confidentiality of personal data and information.

One of the greatest fears of our society is the vast amount of personal information which is being collected by the government, businesses, and other public and private organizations of our society and

²William M. Fuori, Anthony D'Arco, and Lawrence Orilia, Introduction to Computer Operations (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981), p. 6.

³John P. Hayes, Computer Architecture and Organization (New York: McGraw-Hill Book Company, 1978), pp. 16-19.

⁴John A. Stern and Nancy Stern, An Introduction to Computers and Information Processing (New York: John Wiley & Sons, 1982), pp. 506-507.

the potential for the abuse and misuse of this information. This information is collected by the government to maintain the tax rolls, to establish eligibility for entitlement programs, and to perform other necessary governmental functions. Businesses need to collect this information to comply with federal and state regulations; they also collect information to conduct their normal day-to-day activities. For example, management uses this information to determine which employees receive promotions or raises. In many cases, the collection of this information is mandated by law. However, many people consider the collection of information as an unwarranted intrusion into their private lives and business.

The right to privacy and to protection from unreasonable searches and seizures is ingrained in our national psyche. This right is protected by our constitution, and many people in our country fear this right is being undermined by the computer. When data was collected and processed manually, the abuse and misuse of the information produced from this data was very limited; it was difficult to amass large amounts of data on individuals and to process it. Although it was not an impossible task, in many cases the time and expense required to process the data was prohibitive. The modern computer with its sophisticated software has largely removed this constraint and has made it easier to amass large information files on many individuals.

However, two recent developments have had an even greater influence on the citizens' fear of the invasion of their privacy. These two developments are the rapid growth in telecommunications, more specifically, the computer networks and the ubiquitous micro-

computer.⁵ While this has enabled businesses and government to be more efficient, it has enabled both to obtain information which would have been unobtainable in the past or only obtained at great expense. Furthermore, due to the relatively low cost of the microcomputer, the equipment and software, many private citizens are purchasing this capability. This has further increased the fear that information kept by many organizations is in danger of being compromised and used for purposes for which it was not intended. This feeling was reinforced by the Watergate scandal.

In the aftermath of the Watergate scandal, Congress enacted two laws--the Privacy Act of 1974 and the Right to Financial Privacy Act of 1979.⁶ The Privacy Act of 1974 deals with the information collected and maintained by federal agencies on the individual. The law states that the agency must obtain written consent from the individual before it can release the individual's information. However, the agency does not need to obtain the individual's written consent for information obtained through the legal process, such as a court order. Also, the individual has the right to inspect his or her personal information and to correct any erroneous information. The Right to Financial Privacy Act of 1979 deals with the information that a federal agency can collect from a financial institution. Unless the information is obtained under the legal process, the agency must notify the individual prior to obtaining this information.

⁵Stern and Stern states (Introduction to Computers and Information Processing, p. 267) "there were over 250,000 microcomputers sold in 1980, and the predictions are that, by 1985, 3.8 million personal computers will have been sold. . ."

⁶Stern and Stern, Computers and Information Processing, p. 517.

Even before the Watergate scandal, there were laws passed to protect the privacy of the individual. One of these laws was the Fair Credit Reporting Act of 1969.⁷ This law allows the individual to review the personal credit information that has been collected by various credit bureaus and provides the individual the opportunity to correct any erroneous credit information.

Public and private entities collect and maintain data, other than just personal data. These are the organizational data of the entity. These data are as important, if not more important, than personal data. These other data are financial, inventory, marketing, etc. These data are important because, after processing, it (1) provides the management with the necessary information to manage the organization, (2) satisfies government reporting requirements, which are mandated by law or regulation, and (3) provides information to attract new investors or contributors. To be of value, this information must be timely, accurate, and pertinent. Also, the data and the information produced from the data has an intelligence value. For example, research and development data and/or information about a new product could have an industrial intelligence value to domestic and/or foreign competitors.

Therefore, an organization must provide the same level of protection for its data and information resource as it does for its other resources. Also, much of this data and information is recorded on a media that can only be read or used by special equipment, for example, computers, microfiche readers, etc. An organization must protect this equipment as well.

⁷C. C. Gotlieb and A. Borodin, Social Issues in Computing (New York: Academic Press, Inc., 1973), p. 78.

Each organization is responsible for determining and implementing its own data and equipment security measures. These security measures can only be as effective as management desires. Like everything else, costs, both tangible and intangible, are involved in implementing and supporting various security measures. It is the responsibility of each organization to balance the costs of various security measures against the costs of having the data compromised, the software altered or destroyed, or the equipment damaged or destroyed.

In order to have a viable information system, one needs not only the data but also the hardware and software to process it. But what is an information system? An information system is the collection of people, procedures and equipment designed, built, operated and maintained to collect, record, process, store, retrieve and display information. All information systems, whether business, scientific, hospital, etc., serve the same purpose--to provide information to the users, so they can perform their jobs more efficiently and effectively. The only difference is the type of data that is stored and the type of information produced from the data.

In order for an information system to be viable, it must be adaptable to change. The modifications to the information systems occur, because the organizations are constantly changing in response to the events in their internal and external environments. These changes, which occur in information systems, can be either minor or major. Minor changes are usually associated with routine system maintenance; major changes are usually associated with system projects. Also, minor changes, as a rule, do not require a large expenditure of funds, energy or time; whereas, major changes require just the oppo-

site.⁸

Furthermore, an organization can categorize its information system in any way that is suitable to its needs. Burch, Strater and Grudnitski state ". . .one universally accepted classification scheme of information suitable for all situations does not exist,"⁹ and Teichroew states "information systems may be classified in various ways for various purposes."¹⁰ One type of information system is the hospital information system, which is the focus of this study.

The hospital information system, like all information systems, can be classified many ways. The classification depends on the purpose or on the publication read. A brief description of three of these classifications will illustrate this point.

One classification is given by the American Hospital Association (AHA). The AHA divides the automated information system into six categories: financial information systems, dedicated departmental information systems, hospital information systems, medical diagnosis and treatment information systems, management information systems, and health data information systems. Furthermore, the AHA subdivides the hospital information system into three subcategories: (1) the admissions, transfers and discharge (ATD/registration systems, (2) order entry, message switching, and data collection systems, and (3) medi-

⁸John G. Burch, Jr., Felix R. Strater, and Gary Grudnitski, Information Systems: Theory and Practice (New York: John Wiley & Sons, 1983), p. 35; Stern and Stern, Computers and Information Processing, p. 433.

⁹Ibid., p. 18.

¹⁰Encyclopedia of Computer Science, 1st ed., s.v., "Information Systems" by Daniel Teichroew.

cal data management systems.¹¹

A second classification is given by Marion J. Ball. In this classification, a hospital information system can consist of three systems, which are (1) system coordination, (2) clinical subsystems, and (3) administrative/financial subsystems.¹²

A third classification is given by Charles J. Austin and Melville H. Hodge. In this classification a hospital information system can consist of three systems: (1) the clinical subsystem, (2) the administrative subsystem, and (3) the management subsystem. This is the most common classification of a hospital information system and will be discussed more fully in the next chapter.¹³

To add to the confusion, the term "hospital information system" is not even universally accepted. Some individuals prefer the term "automated hospital information system." Still others prefer the term "medical information system."¹⁴

However, even with the different classifications of hospital information systems and the difference in the use of the terms, all agree that hospital information systems, no matter how they are defined or classified, should provide the means for interdepartmental communica-

¹¹American Hospital Association, Hospital Computer Systems Planning: Preparation of Request for Proposal (Chicago: American Hospital Association, 1980), p. 7.

¹²Marion J. Ball, "The Need for a Hospital Information System," How to Select a Computerized Hospital Information System, ed. and comp. Marion J. Ball (Basel, Switzerland: S. Kager, 1973), p. 11.

¹³Melville H. Hodge, Medical Information Systems (Germantown, Md.: Aspen Systems Corp., 1977), pp. 70-71; Charles J. Austin, Information Systems for Hospital Administration (Ann Arbor, Mi.: Health Administration Press, 1979), p. 11.

¹⁴Hodge, Medical, p. 8.

tions. Furthermore, the basis of the hospital information systems is the patient record.¹⁵ The current trend is toward fully integrated hospital information systems. However, this was not always the case.¹⁶

In the past, many hospital information systems were put together in a piecemeal fashion; this was caused by the inadequate planning by the hospital administrators who did not take into account the human factors involved and who underestimated the staffing needed to operate the automated equipment.¹⁷ Also, the manufacturers overstated the performance standards of their software and equipment; they were unable to provide the service or the support that they had promised. Eventually they abandoned the hospital market and they moved into more lucrative markets. Furthermore, delivery and installation time averaged 1 to 2 years after the system was ordered. The results for the hospitals, that had ordered and installed automated systems, were disastrous. As a result, many hospitals shifted to service bureaus or installed dedicated systems for departmental use. More recently, because of the growth and innovations in computer technology, software, and communications technology, many hospitals are installing their own computer systems. Other factors, such as lower costs, better support and maintenance from manufacturers have played a significant part as well.

¹⁵Kathleen A. Waters and Gretchen Frederick Murphy, Systems Analysis and Computer Applications in Health Information Management (Rockville, Md.: Aspen Systems Corp., 1983), p. 1; Austin, Information Systems, p. 174.

¹⁶Austin, Information Systems, p. 208.

¹⁷Thomas M. Boyle, Jr., "The Changing Computer Industry," How To Select a Computerized Hospital Information System, ed. and comp. Marion J. Ball (Basel, Switzerland: S. Kager, 1973), pp. 3-5.

CHAPTER II

THE HOSPITAL INFORMATION SYSTEM

The hospital is proving to be a very lucrative market for major computer manufacturers and software vendors, and the growth in the next decade will be nothing short of outstanding.¹ Some of these manufacturers and vendors are IBM, Burrough's, Spectra Medical Systems, Technicon, and National Data Communications, Inc. These manufacturers and vendors are now manufacturing and producing very specialized equipment and software for the hospital environment.²

An important area deals with the equipment and the software needed to implement a hospital information system. This information system will vary along a spectrum of dedicated, specialized systems (e.g., clinical laboratory systems) to a totally integrated, hospitalwide information system. The purpose of these information systems is to "...produce information to meet the needs of the management and operations of the organization."³ To state it more succinctly, it means providing the right information to the right people at the right time.

¹Steven A. Huesing, "Hospital Information Systems: An Administrative Perspective," Hospital Information Systems, ed. Roger H. Shannon (Amsterdam: North-Holland Publishing Co., 1979), p. 54.

²Raymond D. Garrett, Hospitals - A Systems Approach (Philadelphia: Auerbach Publishers, Inc., 1973), p. 141, p. 144.

³John G. Burch, Jr., Felix R. Strater, and Gary Grudnitski, Information Systems: Theory and Practice (New York: John Wiley & Sons, 1983), p. 63.

As mentioned in the previous chapter, a hospital information system is composed of three systems. These are the administrative subsystem, clinical subsystem, and the management subsystem. Each hospital with an automated information system has implemented one, two, or all three of these subsystems. The most common hospital information system only consists of the administrative subsystem. Some hospitals have, in addition to the administrative subsystem, a clinical information subsystem. A few hospitals have all three subsystems. The first system to be described is the administrative subsystem.⁴

The administrative subsystem performs the traditional business functions, such as maintaining the hospital inventory, performing payroll accounting, etc. It also performs functions unique to the hospital, for example, maintaining the bed census.

The administrative system consists of the following subsystems:

1. Facility utilization and scheduling systems.
2. Financial information systems.
3. Materials and facilities management systems.
4. Personnel data systems.

The facility utilization and scheduling systems are used to monitor occupancy rates, clinic and emergency room activity, utilization of individual service facilities (e.g., operating room), and provide a means to efficiently allocate the resources of the institution. These systems are also used to project the average length of time a patient will stay in the hospital, maintain historical data for projections and other uses, maintain census data, to provide patient appointment schedules for

⁴The descriptions of the three subsystems are from Charles J. Austin, Information Systems for Hospital Administration (Ann Arbor, Mi.: Health Administration Press, 1979), pp. 161-178, pp. 185-200, p. 205.

physicians, and provide scheduling of personnel and other administrative functions.

The financial information systems were the first systems used in hospitals. These systems are mainly used for payroll accounting, accounts receivable processing, accounts payable processing, and preparation of financial reports. Another function performed is the allocation of overhead costs and costs from nonrevenue producing activities to various cost centers within the medical facility.

The materials and facilities management systems are used for automating the hospital purchasing, managing the food service area, energy management, project scheduling of the physical plant, and inventory control. These systems can also be used to more efficiently schedule preventive maintenance of biomedical equipment and other equipment located in the hospital, schedule maintenance personnel for more effective and efficient utilization of the people resource, and to exercise better control of construction and remodeling projects through the use of PERT charts, etc.

The personnel data systems are used to maintain employee records, provide various labor reports, provide employee productivity and quality control reports, maintain an inventory of specialized skills and employee certifications, and other personnel matters. Because personnel costs usually comprise 60-70 percent of a hospital's budget, this is one of the most important systems maintained on hospital computer systems.⁵

While the administrative systems provide hospital management with

⁵Ibid., p. 198.

operational information, it does not help the medical facility in performing its primary task, providing health care to its patient population. As a result, some hospitals have implemented a clinical subsystem to aid in this function.

The clinical subsystem maintains the automated patient records, provides for the retrieval of patient records, provides information for the medical audit, and performs other functions necessary for primary patient care. It also consists of special computerized equipment, for example, Computed Axial Tomography (CAT) scanners, computerized monitors for monitoring the vital functions of critically ill patients, and other specialized equipment used in the treatment of patients.

The clinical information system consists of the following subsystems:

1. Automated history system.
2. Computer aided diagnosis system.
 - a. Direct signal processing subsystem.
 - b. Clinical decision subsystem.
3. Computer aided treatment and follow-up system.
 - a. Computer generated treatment protocol and reminder subsystem.
 - b. Radiation treatment planning subsystem.
 - c. Patient follow-up subsystem.
4. Patient monitoring system.
5. Laboratory information systems.
6. Medical records indexing and retrieval system.
7. Pharmacy information systems.

The automated history system involves a two phase operation. The first phase is where the patient answers a series standardized of questions with a "yes" or "no" answer. In the second phase, the patient has a personal interview with a physician who has a printout of the patient's answers to the questions asked by the computer. Thus, according to Austin, "...the physician's time is economized, and he or she can focus on specific problems for which additional information is

needed.⁶ The data collected serves two purposes; the first is to help the physician in patient follow-up, and second is to provide standardized data for medical research.

The computer aided diagnosis system is comprised of two subsystems. They are the direct signaling processing subsystem and the clinical decision subsystem. The direct signal processing system is a monitoring system. An example of the use of this system is the taking of EKG's (Electrocardiogram). The system would function in the following fashion. The signals from the EKG are sent to the computer, which converts the analog signals to digital signals. These signals are processed by the computer and produce a waveform generated by the patient, and the patient's waveform is compared against a known standard. The computer will print out a differential diagnosis from a series of program decision rules. This printout will go to the internal medicine physician for evaluation. It should be noted that the computer is not replacing the physician but is only one of the many diagnostic tools for the physician's use.

The clinical decision system is mostly an experimental system. This system has a data base which groups symptoms related to known diseases and will tell the physician how to confirm a diagnosis with the minimal number of tests. This system will also provide a precise description of differential diagnoses for teaching purposes. Another item provided by this system is a checklist for difficult differential diagnoses and the relevant tests needed to confirm the diagnosis. Finally, this system will collect and provide data for research.

⁶Ibid., p. 165.

It should be noted that the direct signal processing subsystem is currently in use by some hospitals. The automated history system is in limited use, but the main problem is not technical but human. Because they feel that it is too dehumanizing, people dislike dealing directly with the computer. Also, some physicians are resistant, because they feel that the computer is there to replace them. The computer aided diagnosis system is still experimental and has many limitations. The two most important limitations are (1) it is very complex to design and (2) it is extremely difficult, if not impossible in some cases given the current state of technology, to universalize current medical knowledge into standardized mathematical-logical models, which is the underlying base of this experimental system.⁷

The computer aided treatment and follow-up systems are divided into three subsystems. These are the computer generated treatment protocol and reminder system, the radiation treatment planning system, and the patient follow-up system. The treatment and protocol reminder system generates reminders to physicians and nurses about treatment planning and medical and nursing care tasks. The system maintains automated nursing care plans which can be evaluated and used for a quality audit by supervisory nursing personnel. Also, these plans can be used to prepare detailed nursing care orders and to prepare a list of medications to administer to patients. The radiation treatment planning system is used for the preparation and evaluation of individual patient treatment plans; this system is also used to compute the exact dosage of radiation at treatment sites, which minimizes exposure to

⁷Ibid., p. 167.

healthy regions of the body. It also tracks data to permit easy periodic reevaluation of the effects of radiation treatment on the patient. The patient follow-up system generates automatic follow-up reviews and treatment reminders. An example would be the maintenance of a tumor registry, which would automatically generate a notice to a patient for a follow-up visit and would also generate research data for the researcher.

The patient monitoring system is used to monitor the vital signs of the patient and to provide physiological data. This system performs four functions. First, it converts analog signals to digital signals. Second, it stores this data for later retrieval. Third, it provides enhanced measured data through structured analysis of the clinical data based upon programmed decision rules and notifies medical personnel if an abnormal condition is detected. Fourth, it maintains trend data for research purposes.

Laboratory information systems are one of the most common. They can consist of two divisions; these are lab automation systems and lab processing systems. The lab automation systems consist of lab instruments connected to a computer which performs the calculations normally performed by the lab technicians. These computations determine the peak values of tests and determine the concentration of an unknown patient sample. The results are stored and printed. The lab data processing systems can be used independently or in conjunction with the lab automation systems. These systems record test requisitions, schedules of specimen collection and test processing, record the results of completed tests, prepare test reports for nursing units and out-patient departments, prepare summary reports for all tests given to

a particular patient, prepare statistical reports for the laboratory, provide record keeping for quality control and administrative control of laboratory operations, and place the number and type of tests given to a patient in a central file for pricing and billing.

The medical records indexing and retrieval system maintains a continuous history of the treatment that a patient has received and is available if the patient returns for further treatment. It also provides working documents for the medical audit and for the utilization reviews by members of the medical staff. It also serves as the basis for research studies. This system also keeps track of the location of a patient's medical record and the completion status of the record. The system will generate a notice to the attending physician for any final diagnostic and treatment information needed to complete the patient record. The indexes used to retrieve the record can be a patient number, a disease classification, etc. When used by an online retrieval system, an abstract of the patient's record can be displayed on a CRT or printed in the emergency room, outpatient clinics, or admitting departments. Items usually included in the record abstracts are a resume of the patient's medical history and treatment, drug sensitivities, allergies, and other appropriate medical information.

The pharmacy information systems maintain records to control the ordering, stocking, and distribution of drugs and medications. These systems help avoid medication errors and automatically generate patient charges for billing purposes. In addition, these systems can be used for inventory control and to maintain the hospital formulary and other functions deemed necessary by the hospital staff.

The administrative and clinical subsystems have been discussed as

individual units. While not stated explicitly, it has been implied that these two subsystems have their own separate files. When these files are integrated into a common database, the management subsystem has been implemented.

The management subsystem, which is also called a Management Information System (MIS), provides hospital management with the necessary information for planning, controlling, and making decisions. This system is usually viewed as a fully integrated, hospitalwide system which enables the various hospital areas to communicate with each other through CRT's or other peripheral devices. In order for this system to function, a fully integrated data base management system (DBMS) is needed. It should be noted that this is mainly a theoretical concept and a "true" hospitalwide system does not exist.⁸

Some hospitals have successfully implemented parts of this type of system. Where these systems have been implemented, they serve three functions. First, it helps management to make long-range strategic decisions. Second, it provides all levels of the organization with information. Third, it relieves the hospital's personnel from routine and mundane tasks, such as payroll processing and patient test orders. Even on this scale, these systems require a great deal of planning, coordinating, and funding. However, because of financial restrictions or the diversification of the type of data various departments collect, it is not always possible for a hospital to implement this type of system.⁹

⁸Mari Malvey, Simple Systems, Complex Environments, (Beverly Hills: Sage Publications, Inc., 1981), p. 70.

⁹Stephen L. Priest, Managing Hospital Information Systems (Rockville, Md.: Aspen Systems Corp., 1982), pp. 3-4.

Finally, the hospital management must implement effective security measures to protect not only their data but also the software and equipment that processes it. Effective measures must also be implemented to protect the hospital's information on documents, microfiche, and other types of media; also, any specialized equipment (e.g., microfiche readers) must be protected as well. Chapter 3 will give the reasons why data and computer security is important. In Chapter 4 the various methods that one can use to achieve this security will be presented.

CHAPTER III

THE NEED TO PROTECT COMPUTERS AND DATA

When computers were first introduced, data, software, and computer security was nonexistent. The reason for this was that the first computers were used and programmed mainly by scientists and engineers. The technology was open, and there was no protection for trade secrets or assets. At this time, programs and technology was freely exchanged and traded among the technical community.¹

In the early 1960's management became aware that data, software, and equipment were valuable assets and needed to be protected. However, it was the Watergate scandal that placed a major impetus upon the protection of data, software, and equipment.² Then in 1973 the exposure of the Equity Funding insurance fraud, which netted the perpetrators more than \$2 billion, provided even more incentive for data and computer security.³

These events led to the passage of the Federal Privacy Act of 1974 but not to the passage of a federal law which deals specifically with computer crime. However, there are forty sections of Title 18 of

¹Donn B. Parker, Computer Security Management (Reston, Va.: Reston Publishing Company, Inc., 1981), p. 11.

²Ibid., p. 11.

³John A. Stern and Nancy Stern, An Introduction to Computers and Information Processing (New York: John Wiley and Sons, 1982), p. 513.

the United States Code which can be used to prosecute crimes of this nature on the federal level. Also, there are provisions in Title XX of the Financial Institutions Regulatory and Interest Control Act of 1978 that can be used to prosecute individuals for computer crimes. Finally, there are various other federal laws which can be used to prosecute individuals or organizations for computer abuse and crimes (e.g. The federal copyright laws, federal communications law, etc.).⁴

Since 1974, only ten states have passed laws which deal specifically with computer crime. The states which have these statutes are Arizona, California, Colorado, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, and Utah.⁵ The laws in these states vary in both scope and intent. For example, some states protect data that is stored only in the computer; other states protect data that is not only stored in the computer but also stored on auxiliary storage (e.g., magnetic tape). Also some states protect data transmitted over communications lines. Other states do not provide for this protection in their laws. Next, some states, but not all of them, make it a crime to gain unauthorized access to a computer system. Finally, one major weakness of these laws are the statutory definitions. According to Parker ". . .it is important when applying any computer crime law to read the definitions carefully because they differ from law to law, and statutory definitions differ from common usage in the computer field."⁶

With respect to the medical field, some states have passed laws

⁴Parker, Computer Security, p. 101.

⁵Parker, Computer Security, p. 97; Stern and Stern, Computers and Information, p. 512.

⁶Parker, Computer Security, pp. 100-101, pp. 210-228.

which deal specifically with the medical records of individuals. These laws deal with protecting the confidentiality of patient medical records and allow the patient to have access to his or her medical records to examine them, to make corrections to them, or to make additions to them.⁷ These laws vary in scope and intent from state to state, and each state defines a medical record differently as well. In some of these states, medical records are defined to be specialty records (e.g., medical records in psychiatric facilities). In other states, medical records are single reports (e.g., patient histories or emergency reports). The states with these laws are Alaska, California, Colorado, Connecticut, Florida, Hawaii, Illinois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nevada, New York, Ohio, Oklahoma, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Virginia, Washington, and Wisconsin.⁸

In addition, all employees who have access to medical records have been taught to respect the patient-doctor relationship, to respect the confidentiality of the information exchanged between the physician and the patient, and to adhere to the ethical aspects regarding the release of patient information.⁹ Unfortunately, because of mistakes, neglect, or acts of omission, medical records personnel do not always adhere to the standards designed to protect the confidentiality of medical information.

⁷Kathleen A. Waters and Gretchen Frederick Murphy, Systems Analysis and Computer Applications in Health Information Management (Rockville, MD.: Aspen Systems Corp., 1983), p. 335.

⁸Ibid., p. 335.

⁹Ibid., p. 332.

Finally, all accredited medical facilities are required to maintain their medical records according to standards of the Joint Commission on the Accreditation of Hospitals (JCAH). These standards are recognized throughout the health care community and apply not only to manual records but also to automated records.

Because of these events, the press stories about computer crime, and the various federal and state laws which have been enacted, individuals are concerned about the protection being given to their personal data and information. Also, the management of organizations is concerned with protecting the confidentiality of the personal data and information that they possess. Management is also concerned with protecting the confidentiality of organizational data and information as well.

But nowhere is the need to protect the confidentiality of personal data and information felt more strongly than in the health care facilities. The reason is the increasing demands by insurance companies, prospective employers, law enforcement agencies, and other entities for medical information. Furthermore, health care institutions must deal with a myriad of rules, laws, and regulations that govern what medical information can be released, to whom it can be released, and under what circumstances it can be released. These institutions are also under a great deal of public pressure to protect the confidentiality of patient medical information.

Also, there are various federal and state regulations which pertain to medical institutions. These regulations pertain to utilization reviews, utilization review statistics, and other aspects of medical care

given and received.¹⁰ The information for these reviews and statistics is ". . .to produce lists of medicare and medicaid patients requiring admission certification and extended stay certification in compliance with federal regulations."¹¹ Loss, destruction, or alteration of this information could result in lost revenue for the hospital and the possibility of civil or criminal penalties. Hence, the need to protect the data collected, maintained, and processed by the clinical subsystem.

In addition to complying with various laws, rules, and regulations, the medical organizations must protect themselves from three basic threats. These threats arise from natural disasters, internal threats, and external threats.¹² Natural disasters include fire, water damage, "acts of God," such as tornadoes and hurricanes, and various miscellaneous events, such as explosions.

Internal threats can be subdivided into those threats which are accidental and those threats which are deliberate. Examples of accidental threats are human errors or machine malfunctions; examples of deliberate threats are vandalism, embezzlement, or fraud. External threats include the disruption of computer services or the stealing of data or information by outside parties.

Natural disasters are typically very damaging and very expensive. The most common natural disaster is fire.¹³ Water that is used

¹⁰Charles J. Austin, Information Systems for Hospital Administration (Ann Arbor, MI: Health Administration Press, 1979), pp. 175-176; Waters and Murphy, Systems Analysis, p. 73.

¹¹Austin, Information Systems, pp. 175-176.

¹²Bruce J. Walker and Ian F. Blake, Computer Security and Protection Structures (Stroudsburg, PA: Dowden, Hutchinson & Ross, Inc., 1977), p. 1; Parker, Computer Security, p. 1.

¹³Walker and Blake, Computer Security, p. 2.

to fight the fire can, in some cases, cause more damage than the fire itself. Other sources of water damage are broken water pipes and floods. Currently most sprinkler systems in the computer room contain Halon, which is more commonly known as Freon. Its only disadvantage is that it is a toxic substance in concentration of over 15%, which can present a danger to personnel in the computer room.

Besides protection against natural disasters, an organization must take steps to guard against accidental threats. One source of accidental threats are human errors or omissions.¹⁴ Human errors result in the loss or destruction of printouts, punched cards, and source documents. Also, computer operator errors must be taken into account. Operator errors consist of mislabeling magnetic tapes, accidental erasure of magnetic tapes or disks, restarting the job at the wrong restart point, etc. These errors result in lost time and money to recreate the desired information, which in a few cases may be impossible, because the source documents no longer exist or it is not economically feasible.

Another source of accidental threats are machine errors or malfunctions. Machine errors and malfunctions can result from air conditioning failures, from fluctuations of line voltages, from power failure, etc. The result is the loss or destruction of data and the production of erroneous information. Machine errors can also be caused by the communications paths used by the computer. The causes of communications errors are noise, crosstalk and other physical characteristics of the communications lines.¹⁵

¹⁴Ibid., pp. 3-4.

¹⁵Kenneth Sherman, Data Communications: A Users Guide (Reston, VA.: Reston Publishing Company, Inc., 1981), pp. 199-202.

Software or programming errors can be the result of a human or machine error. A hardware error could result in bad data which causes the program to terminate abnormally. A programming error, commonly called a "bug", can also result in abnormal program termination. A more insidious type of error occurs within this realm. A program may not terminate when it receives invalid data, or it may ignore valid data. In other words, the program runs successfully and produces incorrect or useless information and gives no indication that an error occurred or where the error occurred in processing.

Another potential problem in the software area involves the operating system. This program controls the computer and performs many routine housekeeping functions that a programmer would otherwise have to perform, such as handling machine input and output. The problem arises from the "trapdoors" that exist in the operating system. These trapdoors are the result of code that is placed in the operating system, so the vendor can debug this program to insure that it is functioning properly. After all testing is completed, the vendor will remove these trapdoors; however, sometimes they are overlooked and remain in the operating system. If a programmer can find these places where the code had been deleted, he or she could then place their own code in the operating system. This programmer-inserted code is often called a "trojan horse," which means that this code allows the operating system to function normally until some predefined conditions are detected and then this covert code is executed. To make matters worse, this code can erase itself after it performs its illicit function. With this code a programmer can take over a computer for his or her own purposes or can cause a great deal of damages as the following example will show:

An employee who was dismissed from his job placed a digital 'time bomb' in the firm's computer. Six months later the company's accounts receivables file was completely destroyed. Since the firm was unable to recreate this file and was unable to determine who owed them money, the firm did not have the necessary cash flow to pay its creditors and had to file for bankruptcy.¹⁶

An organization must also guard against deliberate threats. Threats in this area are the willful destruction of equipment, data, and software. Another threat is the embezzlement of funds, the passing of confidential information and data to outside sources, and other criminal acts. A few actual examples will serve to illustrate this point.¹⁷

1. An emotionally disturbed programmer at a major pharmaceutical company destroyed computer records with a powerful magnet. It took the company months to reconstruct the files.
2. An employee who was angered about being dismissed from his job deliberately erased some vitally needed programs used by his employer.
3. Some students at the University of California at Berkeley tapped into the university's computer. They removed, altered and destroyed the information that it contained.

The final area is threats from external sources. These threats can cause the disruption of computer services by striking employees or disgruntled individuals who have a grudge against the organization. Also, these threats can be caused by individuals who, for their own reasons, want to steal, alter, destroy, or modify data, software, or equipment. A few actual examples will serve to illustrate this point.

1. A man was indicted for using his home computer to gain credit card information on 80 consumers. He then charged \$50,000 worth of computer equipment and other

¹⁶Michael Schrage, "Computer Chips in on Crime," Washington Post, Sec. D, p. D8-D-9.

¹⁷Fredda Sacharow, "Computer Criminals: A New Breed," New York Times, 4 April 1982, Sec. 21, p. 1.

electronic equipment to these individuals' accounts.¹⁸

2. By using a computer in a major brokerage firm, a former Federal Reserve Board aide gained access to the sensitive automated files of the FED. The former aide was able to gain access to the Federal Reserve Board's computer, by using another Fed employee's name and password.¹⁹

While not all these examples pertain to the health care industry, they do represent the need for a viable security program to be implemented and enforced in the medical facilities. It would be well within the realm of possibilities for hospital funds to be embezzled, for narcotic medications to be obtained through fraud, or patient information to be obtained for blackmail or other illicit purposes.

Therefore, it behooves hospital management to define the necessary security measures and policies and to provide penalties for non-compliance by hospital personnel. The security measures adopted will vary depending upon how extensive the hospital information system is. For example, if only the administrative subsystem is implemented, then the security measures would be mainly concerned with protecting the hospital's financial data. If the clinical subsystem is implemented, then the security measures will be concerned with protecting the confidentiality of patient information. Finally, if the management subsystem is implemented, then the security measures, which are adopted, will have to provide protection for all the data contained in the hospital's integrated data base.

This is only a small portion of the threats that all organizations

¹⁸ Philip Smith, "Fairfax Man Charged with Tapping Files by Computer," Washington Post, Sec. B, p. B1.

¹⁹ Al Kamen, "Fraud Charged in Fed Computer Case," Washington Post, 5 January 1983, Sec D, p. D1.

face. There are many other threats which all organizations must deal with and resolve. The protection and security measures that the organizations can adopt and implement will be discussed in the next chapter.

CHAPTER IV

THE METHODS OF PROTECTION

In the previous chapter, the reasons for protecting data, software, and equipment were given. In this chapter, the various methods for protecting these resources will be given. A strong commitment by all levels of management--especially upper management--is the key element in implementing and maintaining a successful and viable security program.¹

To obtain management's commitment to a security program, it should be presented in the form of an investment decision. This means that the costs which the organization will incur from the loss, alteration, modification, or destruction of the data, information, software, or equipment should be compared to the costs incurred by implementing the security measures. Also, the effectiveness of the security measures need to be presented. In preparing the costs for the security measures to be adopted, three things need to be considered. These are (1) the value of the information, (2) the assessment of the threats, and (3) the cost of the security measures and their effectiveness.²

¹Thomas J. Knapp, "Selling Data Security to Upper Management," Data Management, July 1983, p. 22; Donn B. Parker, Computer Security Management (Reston, Va.: Reston Publishing Company, Inc., 1981), p. 26.

²David K. Hsiao, Douglas S. Kerr, and Stuart E. Madnick, Computer Security (New York: Academic Press, Inc., 1979), p. 59.

All information has a value to the organization. The determination of this value, however, is subjective in nature. It is obvious that non-critical information will have a low value and critical information will have a high value. The problem is determining which information is critical and which information is non-critical.

The assessment of threats is the second element which must be evaluated. The cost of these threats is determined by risk assessment. That is, the cost of a threat is determined by multiplying the probability that the threat will occur times the cost of the loss or destruction of the resource. For example, if a microcomputer costs \$5,000 and the probability that it will be stolen is .10, the cost of this threat is \$500. This means that management would not want a security measure or measures that cost more than \$500. The organization's management must perform this analysis for all threats that they feel are likely to occur.

Threats can be either intentional or unintentional. Most organizations are more concerned about the losses from intentional threats than they are from unintentional threats. However, according to Hsiao, Douglas, and Madnick "...the unintentional threat may be the most frequent and possibly have a greater overall economic impact."³

The final element in determining cost is the cost of the security measures and their effectiveness. The more effective the security measure, the more it costs. Therefore, the cost of the security measures should not exceed the cost of the loss or destruction of the resources they are designed to protect.

³Ibid., p. 62.

A viable security program should accomplish three things. The first is to minimize the probability of an event from occurring; this means implementing measures which are preventive in nature. The adoption of fire prevention measures is an example of a preventive measure. The second element should be to minimize the damage if the preventive measures should fail. An example of this would be to discard a disk pack that has been dropped and damaged. This would prevent the defective disk pack from being mounted on a disk drive and possibly damaging the disk unit's read/write heads. The final element is to design a method to recover from the damage. For example, the organization may preserve certain source documents to reconstruct a file that was lost or damaged. Another method to recover from the damage to important or sensitive data, information, and software is to have a duplicate copy (backup) of these items.⁴

To protect the confidential data and computerized records of the organization, four types of security are needed. These are (a) physical security, (b) software security, (c) data security, and (d) Psychological (people) security.⁵

The first area of concern is physical security. Physical security is comprised of two parts--protection against natural disasters and measures taken to restrict access to computer equipment.⁶ Natural

⁴James Martin, Security, Accuracy, and Privacy in Computer Systems (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1973), p. 11.

⁵Harry Katzen, Jr., Computer Data Security (Von Nostrand Reinhold Company, 1973), pp. 4-5; Charles F. Hemphill, Jr. and John M. Hemphill, Security Procedures for Computer Systems (Homewood, Ill.: Dow Jones-Irwin, Inc., 1973), pp. 6-7.

⁶Hsiao, Kerr, and Madnick, Security, p. 93.

disasters consist of fire, tornadoes, and other "acts of God." Site selection and preparation is one of the most important considerations in physical security. Buildings should not be built in floor plains, near fault lines, etc. In addition, buildings should be built of reinforced material if located in areas susceptible to hurricanes or other extremely violent storms. Also, since fire is the most common natural disaster, buildings should be constructed of flame-retardant materials, should have smoke detectors installed, and should contain fire extinguishers with carbon dioxide. Finally, precautions should be taken to prevent damage from power surges or failures. The best way to protect against power fluctuations is to install backup generators and surge depressors. To obtain protection from a disastrous loss, the company should purchase insurance.

The second area of physical protection is to guard against intruders. This second area is often called access control, and it can be divided into four subdivisions.⁷ Hsiao, Kerr, and Madnick call these four subdivisions "...boundary protection (the area outside a building), perimeter protection (the building itself or barrier around it), entrance protection, and critical-area protection." Martin also subdivides this area, but he terms his division as "levels" or "layers of protection."⁸

There are a number of methods which can be used to implement this type of security. These measures can be very simple, or they can

⁷Bruce J. Walker and Ian F. Blake, Computer Security and Protection Structures (Stroudsburg, Pa.: Dowden, Hutchinson & Ross, Inc., 1977), p. 23; Encyclopedia of Computer Science, 1st ed., s.v. "Security of Computer Installations, Physical" by William F. Brown and R. V. Jacobson.

⁸Hsiao, Kerr, and Madnick, Security, p. 96; Martin, Security, Accuracy and Privacy, p. 278.

be very sophisticated. For example, one method of securing the facility would be to erect an elaborate network of fences. Obviously, this method would not work for a hospital, where easy access is not only a requirement but a necessity. Another practical method for hospitals is to have security guards and well lit areas.

Another method of protection would be to have the computer and its related items in an area where there are few windows or non-secure openings. Inside the facility there should be only one entrance point where personnel, who enter the area in which the computer equipment is stored, can be monitored. The diagram on the following page (Figure 4.1) shows a suggested layout of a computer facility. The offices are used by the manager and assistant managers. The Field Engineer (F.E.) office is for the computer maintenance technician. The production control area is where the users bring their input for batch processing and receive their output for jobs that have been processed. This facility is usually located in the basement, the upper floor of a building, if feasible, or in a separate building. Note there are very few entrances, and it is easy to monitor and control access to the facility.

Also, a passive device, such as a sign stating "authorized personnel only" or "employees only," is also a very practical method of protection. However, more sophisticated devices could be used, such as closed circuit TV's or electronic locks.

A simplified diagram of an electronic lock is shown in Fig. 4.2 (p. 35). The push buttons are similar to the push buttons found on a touch-tone telephone. This lock functions like a mechanical combination lock; instead of turning a dial, one just pushes the buttons in the

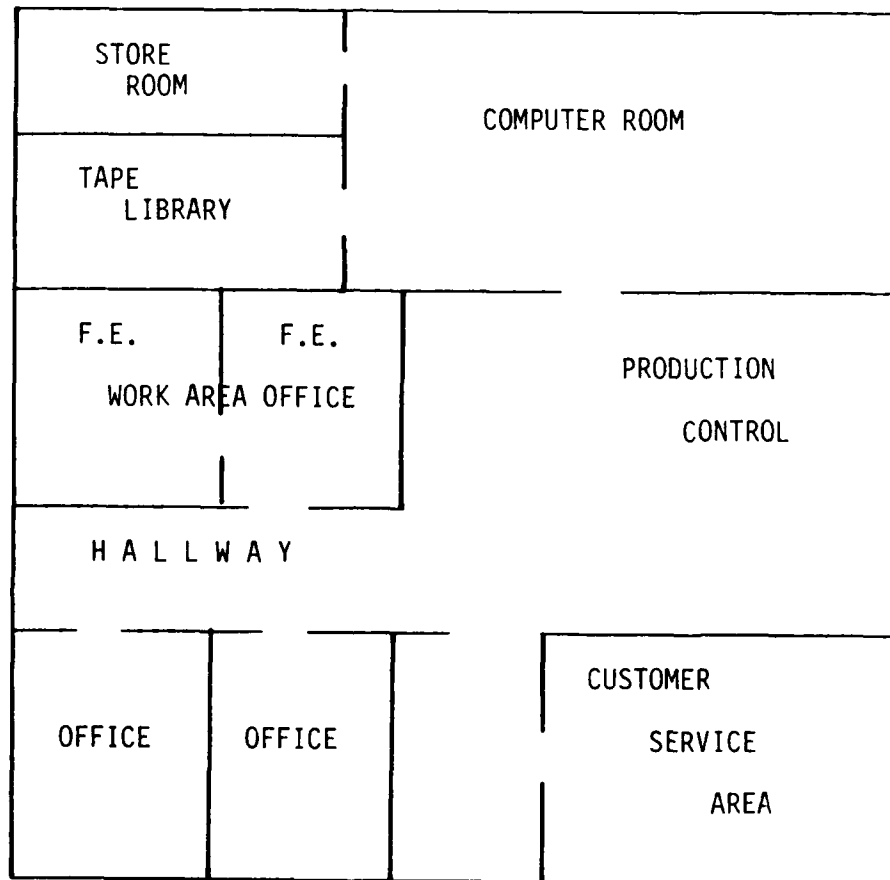


Fig. 4.1 Computer Center Floor Plan

1	2	3	4	5
[]	[]	[]	[]	[]
[]	[]	[]	[]	[]
6	7	8	9	0

Fig. 4.2 Partial Diagram of an Electronic Lock

correct sequence, and the door is electrically unlocked and the individual can enter the area. If the incorrect combination is entered more than once, an alarm is sounded to indicate someone is tampering with the lock, or that an employee forgot the correct combination.

In those systems where remote terminals are used, it is important that the user as well as the terminal be identified. The user can be identified by a password assigned by the data processing facility, or the user can have a dynamic password. A dynamic password is one that changes with time and must be calculated before it is input. The numbers used are based upon personal information known only to the user. For example, to calculate the dynamic password, the user may have to multiply his birth month and day times his wife's birth month and day. He would then take the product and divide it by the current day. The quotient would be the password he would use for that day.

Another method of assuring system security is to have the host computer system check the terminal ID. If the terminal ID is not one known to the host system, then the host system can automatically disconnect the device that is attempting to gain access to the computer system. In Chapter III an example was given in which a man accessed a credit card company's computer by using his home computer. If the credit card company's computer had been programmed to check for the terminal ID, the man who committed the fraud possibly would not have been able to get access to the credit card files.

One final item in the area of physical security is electromagnetic radiation. This occurs when electric circuits are arranged to display information on a cathode ray tube (CRT). The stray electromagnetic radiations might be amplified to produce the same image on another CRT that has no connection to the first. One method of protection to guard

against this event is to insure that the CRT's are placed in separate rooms. If this is impossible, then display devices should be separated by 20 feet or more. Another effective measure is to physically shield the devices or circuits.⁹

Software security is concerned with the programs that instruct the computer on what to do and how to do it. Without software a computer is a useless piece of equipment. There are basically two types of software; the first type is the operating system software, and the other type is the user software. The operating system is the master program which controls the computer system and provides many services to user software, for example, input/output operations. User software, also called applications software, is a program or programs written by the users to perform some specific function for the organization.

The best method of protection for all software is to use grandfather, father, son technique. This technique has two copies of the original software made. The original and one copy is stored in the tape library and the other copy is stored in a secure off-site location. This guards against accidental or deliberate destruction of important software.

To protect the operating system, only authorized systems programmers should be allowed to make changes or updates to it. Also, the tasks performed by the operating system should be compartmentalized to prevent any one systems programmer from having total knowledge of

⁹Walker and Blake, Computer Security, p. 57; Hsiao, Kerr and Madnick, Security, p. 99; Encyclopedia of Computer Science, 1st ed., s.v. "Data Security" by J. N. P. Hume.

how the complete operating system functions. This prevents a systems programmer from inserting a "trojan horse" program in the operating system. This technique also mitigates the possibility for a systems programmer to find any "trapdoors" that could possibly exist.

In Chapter III an example was given in which a disgruntled employee placed a "logic bomb" in the operating system. If the company had compartmentalized the operating system, this disgruntled employee may not have known the total operating system. Since he would have known only a portion of the operating system, he would not have been able to place his "logic bomb" in the system.

For application programs, there should be a division of responsibility. This means that no one person should write the whole program. Also, programmers should be rotated to different systems to prevent an individual from learning how a whole system functions. The organization should also establish audit trails to insure that programs function as they should; this is especially important for programs that process accounting data. For a hospital the audit trail should be established for programs that process transactions dealing with medications, especially Schedule II and Schedule III drugs.

Finally, an organization can obtain legal protection for its software. Some of these legal measures are copyright protection, trademarks, licensing agreements, contracts, etc. Copyrights and trademarks are usually easy to obtain and inexpensive. Patents are usually very difficult to obtain and expensive. The patent office is usually opposed to granting a patent on software because it views a program as nothing more than ". . . a 'mathematical theory' or a 'computation' or a

'series of mental steps'. . ."¹⁰

Data security is concerned with the protection of data from accidental or intentional destruction, modification, alteration, or release to unauthorized persons. Data protection methods can range from simple protection schemes to sophisticated protection schemes.

The simplest method of protection and the most common is password protection. The purpose of a password is to identify the user. Furthermore, the password can be maintained in a table that specifies the user's access rights; these access rights specify whether a user has read-only privileges, read-write privileges, or update privileges. Also, as a rule, a user is required to give an account number for billing purposes. The disadvantages of passwords are they can be given away, forgotten, or stolen without the user's knowledge. The theft of passwords can be accomplished by wire-tapping or by obtaining a hardcopy of the output from a terminal. The best method to insure against theft is to frequently change a user's password. This method is used with data that requires only minimal protection.

An additional layer of protection can be implemented by using "lockwords". For example, a user must use a password to gain access to the computer system. After the user gains access to the computer, he or she must input a second password to gain access to a file, data elements, etc. This second password is called a "lockword" because it "unlocks" (i.e., allows access to) various files or data elements, etc. This second password or "lockword" is different from the password used to gain access to the computer. Without this second password the

¹⁰ Encyclopedia of Computer Science, 1st ed., s.v. "Legal Protection of Software" by Calvin N. Mooers.

files, data elements, etc. are inaccessible to the user.

Another method of protection is to maintain logs. These logs should list all the requests by a user along with date and time of the access, the file or program accessed, the terminal ID, and whether the access was granted or not. These logs should be printed periodically and checked for possible security violations and allow management to take the appropriate corrective action. Logs can also be used for recovery purposes. If, for example, data was left in a partially updated state due to a system or program malfunction, the user could be notified of this fact and have a backup of his or her file reloaded. Logs can also serve as a psychological deterrent to intruders.¹¹

Currently, the best method for protecting data is encryption. The purpose of encryption is to make the data unintelligible to a person who does not have the key to decipher the data. Data encryption can be accomplished by either software or hardware. Crypto devices usually use a 64-bit key to encypher data. Thus, if someone tries to break the code by using trial-and-error methods and could try a new key every microsecond (i.e., one millionth of a second), it would take an average of 292,271 years to find the correct key.¹² Data encryption is useful when transmitting data over communications paths (e.g., communications lines, microwave transmission, etc.); it is also useful in protecting sensitive data in a data base.

A corollary to data security is data integrity. If the data and

¹¹Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, N.J.: Prentice Hall Inc., 1977), p. 35.

¹²James Martin, Design and Strategy for Distributed Data Processing (Englewood Cliffs, N.J.: Prentice Hall, Inc., 1981), p. 595.

information stored in the computer system or on other storage media are inaccurate, then the security measures are almost worthless. If users cannot rely on the information produced by the computer, they will not use either the computer or the information. An organization can institute input controls to help insure that the data input into the computer system is correct. The organization can also institute output controls to help insure the information produced from the processed data is valid. Some examples of input controls are hash totals, the proper labeling of input data, and verifying the data before it is input. Some examples of output controls are screen the output for obvious errors, only allow authorized personnel to distribute output products, and reconcile hash totals. Also, the computer can be used to edit input data. For example, the values in certain data fields can be checked to ascertain that they are within an acceptable range; if the values are outside of the acceptable range, the computer can flag the input transaction and not accept it for further processing. The computer can also perform data checks during processing. For example, critical calculations can be performed twice and the results of these calculations can be compared to see if they are equal.¹³

The last method of data protection is physical control. This involves protecting information which is printed on listings generated by the computer or information printed on microfiche. These media should be accorded the same protection as manual files. It also involves storing magnetic tapes and disk packs in a secure room, which

¹³John G. Burch, Jr., Felix R. Strater and Gary Grudnitski, Information Systems: Theory and Practice (New York: John Wiley & Sons, 1983), pp. 451-452, p. 457.

should be separate from the computer room. Access to this room should be controlled by the tape librarian, who should obtain the tapes and disks needed to process a job. It also means that magnetic media should be stored safely from transformers and other devices that produce strong magnetic fields. These magnetic fields can erase or destroy the data recorded on this media. Also, diskettes used with microcomputers should be stored in a locked cabinet or desk with access controlled by the section that owns the system. This is necessary because diskettes are small and can be easily hidden and removed. Like magnetic tape and disks, diskettes need to be protected from strong magnetic fields.

The final area of security is psychological (people) security. This area deals with the management of people who use and operate computer equipment. Employees should understand their responsibilities for protecting the data, information, software, and equipment that is under their control. Also, management should insure that the employees take security seriously and are punished when they violate the security rules implemented by the organization. Also, management has the responsibility to keep morale high. When employees have a low morale, they become careless or disgruntled. If it becomes necessary to terminate an employee, he or she should be removed from the area immediately. This prevents the employee from taking out his or her revenge on the equipment, data, information, or software. Finally, management should set the example for their employees. If management pays only "lip service" to security, then the employees will usually feel that it is "red tape" to be circumvented.¹⁴

¹⁴Martin, Security, pp. 392-396.

The security measures discussed in this chapter are only some of the measures that can be adopted. It should be remembered that no security measure or combination of security measures is foolproof. According to Martin, "Absolute security is unattainable."¹⁵ This means that if an individual is determined to gain access to a computer system, he or she will eventually find a way to bypass the security measures implemented by the organization.

In the next chapter the problems and the deficiencies in protecting the data in hospital information systems will be explored and what corrective measures can be taken to improve the situation.

¹⁵Ibid., p. 7.

CHAPTER V

DEFICIENCIES IN HOSPITAL INFORMATION SYSTEMS

The hospital information system is a complex system that consists of the following information: personal data and information, information about the hospital's employees, important organizational data and information, and patient data and information. The need to protect all this data, information, software, and equipment is vitally important. However, there are deficiencies which can compromise and undermine the security that is needed. So that a hospital's security program can be more effective, these deficiencies need to be recognized and understood. This chapter will discuss these deficiencies and their impact upon data and computer security.

One deficiency is technological. Computer technology is constantly changing at a rapid rate. Inherent to this is the rapidly changing telecommunications field which is also having an impact upon how computer systems are designed and built. This in turn leads to more complex systems which are becoming difficult to manage effectively and efficiently. This problem not only impacts hospital information systems but also all information systems. According to Parker ". . . the human capability to manage the development of complex systems of today is being taxed to the limit."¹ This means that for security

¹Donn B. Parker, Computers Security Management (Reston, Va.: Reston Publishing Company, Inc., 1981), p. 9.

measures to be effective, they must be given a high priority instead of the low priority that they have been given in the past.²

One of the major deficiencies is an inadequate system analysis and design; this appears to be a common occurrence in hospital information systems. Hospital management does not appear to have a master plan to design and implement an information system. Priest has made the following observation: "One approach to computerization is to first retain an in-house MIS staff (or hire outside vendor services), acquire a computer, buy applications, and then determine how they are to be used."³ He also observes that ". . . MIS staffing and hardware and software are sometimes determined solely through vendor recommendations."⁴ Also, Austin states ". . . many hospitals have moved into the development of computer systems without any kind of master plan."⁵ This would imply that data and computer security are not even thought of at all or only considered as an afterthought. For example, inadequate audit trails are established or edit checks are not as comprehensive as they should be, etc.

The reason for the lack of a good master plan is lack of involvement by the hospital administration, specifically the hospital administrator. Huesing notes: "Historically, it has not been absolutely neces-

²Office of Technology Assessment, Computer-Based National Information Systems: Technology and Public Policy Issues, (Washington, D. C.: U. S. Government Printing Office, 1981) p. 82.

³Stephen L. Priest, Managing Hospital Information Systems (Rockville, Md.: Aspen Systems Corp., 1982), p. 22.

⁴Ibid.

⁵Charles J. Austin, Information Systems for Hospital Administration (Ann Arbor, MI: Health Administration Press, 1979), p. 41.

sary for the hospital administrator to be involved in the design and implementation of information systems."⁶ However, Austin states, "The hospital administrator should take direct responsibility for organizing the planning effort."⁷

The lack of involvement stems from a misunderstanding of all the underlying relationships involved in a hospital information system. Huesing observes: "They [the hospital administrators] do not have enough of a knowledge base to be comfortable in the decision-making process as it relates to the complexities of hospital information systems."⁸ The lack of knowledge and involvement by hospital management can result in the design of ineffective security measures or even worse, no security measures being designed at all.

Still, another problem is that many older hospital managers did not receive adequate training dealing with computers, their use, or systems analysis. They must rely on outside sources or in-house technical personnel who are usually inexperienced in hospital information systems.⁹ Many outside consultants do not understand the hospital environment, and therefore, design information systems that may be perfectly acceptable to a business corporation but completely inadequate for a hospital.¹⁰ Austin also implies this is the case. He states "he

⁶Steven A. Huesing, "Hospital Information Systems: An Administrative Perspective," Hospital Information Systems, ed. Roger H. Shannon (Amsterdam: North-Holland Publishing Co., 1979), p. 59.

⁷Austin, Information Systems, p. 41.

⁸Huesing, "Hospital Information," p. 59.

⁹Priest, Information Systems, p. 22.

¹⁰Samuel Raymond, "Hospital Information Systems: A Physicians's Perspective," Hospital Information Systems (Amsterdam: North-Holland Publishing Co., 1979), p. 42.

[the consultant] should possess technical knowledge of systems analysis and computer systems but also should be well informed about hospitals and their functioning.¹¹ The administrator or other members of management do not fully understand the analysis and ". . . further complicate the problem by not understanding the problem by not understanding the time and methods necessary to implement. . . a hospital information system."¹²

Another deficiency in hospital information systems relates to collecting too much data. When a hospital collects too much data, it is usually collecting data just for the sake of collecting data.¹³ When too much data is collected, it is difficult to keep it current and accurate. Updates are not usually timely. As a result, the integrity of the data is not maintained and the information produced becomes questionable at best. This increases the chances that information, which should stay confidential, is released either accidentally or deliberately.

A related problem is maintaining old patient data and information that is no longer needed.¹⁴ Examples of old patient data and information are episodic drug use, venereal disease, pregnancy data, and other similar data and information. This creates two problems. First, the cost involved in storing this data and information and second, and more

¹¹ Austin, Information Systems, p. 41.

¹² Priest, Information Systems, p. 22.

¹³ Charles J. Austin and Harry S. Carter, "Hospital Information Systems and Quality Assurance," Hospital and Health Services Administration 26 (Fall 1981): 47-48.

¹⁴ Kathleen A. Waters and Gretchen Frederick Murphy, Systems Analysis and Computer Applications in Health Information Management (Rockville, MD: Aspen Systems Corp., 1983), p. 331.

importantly, this data and information can be used by unscrupulous individuals for blackmail, revenge, or other illicit purposes.

When hospital information systems are simplistically viewed, they are usually designed in the same fashion. Simple systems usually have adequate security measures. However, there are two potential problems. First, there is little thought given to future developments; second, it will not be useful for long. These two problems will eventually lead to a major redesign of the information system.¹⁵ Since an attempt is made to keep costs to a minimum, it is usually the security measures that come up short.¹⁶

Another problem is the failure to involve the users in the analysis and design of the information system. The result is that the system will fail because the personnel will not use it. In this instance, it doesn't matter how well designed the security measures are; they are worthless.

Also, most data processing departments in the hospital are usually placed under the controller or the chief financial officer of the hospital.¹⁷ The department that controls the computer usually insures that its jobs are processed ahead of the jobs of other departments. Furthermore, the comptroller will assure that his or her data are protected but will not always display the same degree of concern about the data of

¹⁵ Aaron Wildavsky, Forward to Simple Systems, Complex Environments, by Mari Malvey (Beverly Hills, CA: Sage Publications Inc., 1981), p. 15.

¹⁶ Office of Technology Assessment, National Information Systems, p. 82.

¹⁷ Austin and Carter, "Hospital Information Systems," p. 55.

other departments. The data processing activity should report directly to the CEO of the hospital. This will insure the security needs of the hospital are in conformance with the overall security program of the organization. It will also reduce the impression that one area of the hospital is receiving preferential treatment at the expense of another area.

Another problem is sometimes the lack of concern by the hospital management toward security in general. Knapp states: "One of the most critical and difficult roadblocks information processing managers face when implementing a data security program is selling the concept to upper-level management."¹⁸ This means that data and computer security measures are only half-heartedly implemented and not followed very closely.

This occurs because top level management does not ". . . fully recognize the importance of data security project requests."¹⁹ The reason for this lack of understanding is the funding requests are presented in "computerese" and not in common business terms. Therefore, these projects are either underfunded or not funded at all.

When the staff sees that hospital management only pays "lip service" to security measures, then the hospital personnel feel that it is just so much "red tape" to be avoided. This results in a greater increase in the possibility that confidential patient information may be released to unauthorized persons or organizations either accidentally or

¹⁸Thomas J. Knapp, "Selling Data Security to Upper Management," Data Management, July 1983, p. 22.

¹⁹Ibid.

intentionally. Also, the critical organizational information can be released as well. This can also cause many problems for the health care institution.

If management is not fully committed to security, there are other ways in which critical information of the institution can be compromised. For example, if there are display terminals in various areas of the hospital, they can be placed in less than desirable locations. This can result in any one seeing what is displayed on them. It also increases the likelihood for such acts as vandalism or theft.

Another deficiency which exists is the inadequate controls on data processing personnel. Mair states "relatively few hospitals. . . have strong enough controls to prevent internal fraud and embezzlement, or invasion of patient privacy."²⁰ This implies that stronger controls over data processing personnel should be implemented, and these personnel should be given closer supervision.

Since application and system programmers are not closely controlled or supervised, they are more or less left to go their own way. With application programmers, the lack of supervision means that the programmers may not incorporate all the necessary edit checks into their programs, such as checking the reasonableness of data, double checking critical calculations, etc. This increases the chances for the data maintained by the hospital to become corrupted and invalid; any information produced from this bad data is worthless. With system programmers, the lack of supervision can have even greater conse-

²⁰William C. Mair, "Computer Abuse in Hospitals," Hospital Progress 58 (March 1977) p. 61.

quences. These programmers possess the knowledge and technical expertise to modify the operating system. It is possible for these individuals to find trap doors in the operating system and to insert their own code. With this code in place, the system programmer(s) could take control of the computer system. With this control, it would be possible to bypass many of the security measures built into the operating system. Once in control, they could embezzle funds or obtain patient information to use for illicit purposes, such as using the information for blackmail, extortion, etc.

Lack of supervision of computer operators would enable the operators to avoid normal operating procedures. For example, the operators would not maintain the proper logs or not follow established procedures about rerunning jobs. Also, the operators may, for one reason or another, not back up certain critical files. Without the proper backup, it may be impossible to recover certain data or could result in the organization spending an inordinate amount of time in recreating these files.

Also, lack of supervision or proper controls could mean that the necessary audit trails are not established, or if they are, then the operators bypass them either because the operators feel that it is inconvenient to follow them, or they wish to cover up their errors or possible illegal activities.

Controls must also exist in user applications. These program

²¹Priest, Information Systems, p. 123.

²²Ibid., p. 119.

controls insure the protection of data and information in the system. These application controls also insure the accuracy of the data. Priest states ". . .there must be ongoing application control procedures that ensure routine operation of the information system."²¹ This implies that there are inadequate control procedures. As a result ". . .many departments still maintain manual data bases and files in order to have control over certain confidential information."²² Therefore, certain data and information that needs to be in the data base is not there. This missing data and information could lead a physician to make a wrong diagnosis and prescribe the incorrect treatment. This could prove to be fatal to a patient. It is obvious that this impunes the integrity of data. Furthermore, it causes the hospital staff to distrust the computer system and its stored data and information. When an atmosphere of distrust exists, the system is not used. This further aggravates the problem of data and information integrity.

Inadequate control procedures can result in other adverse consequences. For example, it would be possible for a person to generate a false physician order for narcotic medications to the pharmacy. The person could then receive these narcotic medications to support his own drug habit or obtain them for sale on the illegal drug market. Another example would be to generate false invoices from fictitious companies to collect money for products or services which were never delivered or rendered.

Another deficiency involves the selection of equipment. For example, a terminal that would be appropriate for the word processing function is selected for use in the emergency room. This means that the physicians or other emergency room personnel would have to search

the screen for the information they were looking for. In a "life threatening" situation the emergency room personnel do not have the time to search for the information they need or the time to enter data into the system. They, therefore, make up manual records and never bother to use the computer or the information system. Therefore, critical medical data is never entered. This not only compromises the integrity of the data and information but also can result in the improper billing of patients for the treatment they received. It can also have an adverse effect on other automated records, such as inventory records, especially those pertaining to medications and supplies used by the emergency room. This would also apply to other areas where critically ill patients are treated, such as the intensive care unit (ICU), cardiac care unit (CCU), etc.

Another problem involves the equipment which must be located in public areas of the hospital, for example, nursing stations, the primary care unit, etc. When an equipment item, such as a terminal, must be located in one of these areas; adequate protection methods are not taken to protect the equipment or to prevent unauthorized access to the automated files. For example, the terminal is placed in a position where the displayed information can be read not only by nursing personnel but also by any person who happens to be at the nursing station. Also, nurses must leave the nursing station to perform other duties. When no one is present at the nursing station, it is possible for an unauthorized person to gain access to the system to generate false physician orders, to obtain information about patients, or to commit other acts (e.g., fraud, embezzlement, etc.). Also, if the equipment is not secured, there is a greater risk that someone could steal it.

The nursing station was used for illustrative purposes. The items discussed in this paragraph could apply to any public area in the hospital in which equipment is located.

These are only some of the deficiencies that currently exist in hospital information systems. However, these are the major ones and can have the greatest impact upon the success of implementing and using a hospital information system. In the next chapter specific recommendations will be made to alleviate these deficiencies.

CHAPTER VI

CONCLUSION AND RECOMMENDATIONS

This thesis explained why individuals are concerned about the privacy of personal data and information collected and maintained about them. It has also explained the concern about the security measures used to protect this personal data and information. Also discussed were the reasons for protecting organizational data and information; in addition, the reasons for protecting the software and equipment were also reviewed. It was shown how this relates to a hospital information system.

The hospital information system can range from a simple departmental stand-alone system to a fully integrated hospital-wide system. It needs to be realized that information systems and the computers which support them are tools to be used to more effectively and efficiently manage a very complex environment--the health care institution. The information system and the computer are not meant nor will they ever replace the people who work in these institutions.

There were some deficiencies discussed in this thesis. These deficiencies should not be viewed as being critical of the hospital management, the professional staff, or any department of the hospital. It should, however, point out the need for management to consider all facets of their operations before designing and implementing an information system.

In this regard, there are several recommendations that need to be made. First, the most important aspect of any information system is to determine the critical data and information needed and to keep backup copies of this data and information for system recovery and archival purposes. Also, this data and information is needed to comply with the various federal and state laws as well as the rules and regulations of various federal, state, and private agencies (e.g., Social Security Administration, state welfare agencies, insurance companies, etc.).

Also, when the information system is designed, the users should determine what their information requirements are. They should determine what data elements need to be kept and maintained to provide the desired information. The users should also determine how long these data elements need to be kept for archival purposes or to satisfy legal requirements. After the information system is operational, the users need to review their information requirements for currentness. This review will allow them to add new data elements to meet new requirements and to delete data elements that are no longer needed or required.

A second recommendation is to establish a formal training program for hospital administrators and other hospital managers. In the academic community basic courses in data processing and information systems should be required of all individuals majoring in health care administration at both the undergraduate and graduate level. This would provide these individuals with a background to better manage the data processing personnel employed by the hospital. It would also provide the background to deal with outside consultants who would possibly be hired by a hospital to design, implement, or modify a hospital informa-

tion system. Also, managers at all levels of the health care facility should periodically take continuing education courses that deal with information systems.

Next, the computer system should be chosen that will not only meet the current needs of the hospital but also will be able to expand to meet anticipated future needs as well. Also, the peripheral devices should be considered just as seriously as the computer system itself. For instance, terminals used in areas where critically-ill patients are treated should have color monitors and touch sensitive screens. Color monitors would enable medical personnel to find vital patient information on the screen very quickly, because different information items could be in different colors. Another method to quickly locate information on the monitor would be to identify information items by using different graphics characters that would vary in size, shape, and color. The use of touch sensitive screens would reduce the data and commands that would need to be input via the keyboard.

Another advantage to these types of terminals would enable the vital patient information to be retrieved very rapidly and would provide an incentive for the medical personnel to use the system. This would give them a vested interest in maintaining the data and help to insure the integrity of the data in the data base.

Another recommendation is to insure that a viable security plan is implemented by the hospital. All hospital personnel should constantly be reminded of their responsibilities to protect the data, information, software, and equipment under their control. Management itself should set the example and maintain a high security awareness. Lapses in security should not be tolerated and personnel guilty of such lapses

should be punished.

Furthermore, data ownership should be established, and the department made responsible for maintaining the integrity of the data and information under its control. The department should also be held accountable for the equipment under its control as well. This equipment, such as CRT's, should be placed in areas where access to this equipment can be controlled. In addition, this equipment should be protected from both man-made disasters as well as natural disasters. Also, each department should establish who is to have access to what data and information, who should be allowed to update it, and who establishes the appropriate periods to update the data (i.e., daily, weekly, monthly, etc.). All data, information, and equipment should be protected in accordance with the overall hospital security program.

In those cases where terminals must be placed in public areas of the hospital, such as nursing stations, primary care areas, etc., there are various ways to protect the equipment, data, information, and control access to the computer system. One method of protecting the equipment is bolt it to an immovable object, like a counter, or attach one end of a chain to a wall or counter and the other end to the computer, or secure the equipment in similar fashion. This prevents its easy removal. The monitor should be placed in a position that makes it difficult for patients and visitors to see the displayed information. Also the monitors should be automatically erased after a short period of time (i.e., 1 - 3 minutes). The information could be redisplayed by pressing the "Enter" key, a function key, or a specially designated key, such as the letter key "D" for display. Also the terminals should be automatically disconnected from the system after a period of non-use

(i.e., 10 - 20 minutes). This means that the log on procedure would have to be initiated to gain access to the computer system. Another method of protection is use a terminal that requires that an ID card, similar to a credit card, be inserted in the device to use it. If a person tries to use the terminal without inserting the proper ID card, then an alarm should be sounded and the terminal would automatically be disconnected from the system or the keyboard should be locked to prevent use of the terminal. A similar type of terminal uses the picture on a badge with a photograph of the individual to activate the terminal.

These measures and terminals would insure that only authorized personnel access the data base and would prevent false physician orders for medications, and prevent an unauthorized individual from using the terminal to perpetrate a fraud, or to obtain confidential patient information, or to carry out some other illegal or unethical activity.

Another recommendation is to establish the appropriate audit trails to prevent fraud and embezzlement and to protect the confidentiality of patient medical data. To insure that the internal audit is valid, an independent individual not connected with the department should conduct the audit; this audit should apply to all departments, especially the data processing department.

Another recommendation is the data processing manager should be experienced. This means that he or she should not only possess hospital managerial experience but also should have a strong data processing background as well.

Furthermore, the data processing activity should work directly

for the hospital administrator. This will insure the data processing activity serves the whole hospital, and that the priority data processing activities are done in accordance with upper management's desires and not departmental desires.

Next, all requests for funding a hospital information system and the appropriate security measures should be presented in common business terms and not "computerese." This will enable upper management to fully comprehend the purpose of the funding, the benefits to be derived from the information system, and the value of the security measures. If these managers understand what they are funding, there is less likelihood the project will be undercapitalized.

A final recommendation is to insure that only high-caliber people are hired for data processing activities. In this regard, an individual's background should be checked. Also, the hospital should bond these employees to protect itself from accidental or criminal acts which may be committed by these individuals.

BIBLIOGRAPHY

- American Hospital Association. Hospital Computer Systems Planning: Preparation of Request for Proposal. Chicago: American Hospital Association, 1980.
- Austin, Charles J. Information Systems for Hospital Administration. Ann Arbor: University of Michigan, 1979.
- Austin, Charles J. and Carter, Harry S. "Hospital Information Systems and Quality Assurance." Hospital and Health Services Administration 26 (Fall 1981): 42-62.
- Ball, Marion J. "The Need for a Hospital Information System," How to Select a Computerized Hospital Information System, Edited and compiled by Marion J. Ball. Basel, Switzerland: S. Kager, 1973.
- Boyle, Thomas M., Jr. "The Changing Computer Industry," How to Select a Computerized Hospital Information System. Edited and Compiled by Marion J. Ball. Basel, Switzerland: S. Kager, 1973.
- Burch, John G., Jr.; Strater, Felix R.; and Grudnitski, Gary. Information Systems: Theory and Practice. New York: John Wiley & Sons, 1983.
- Encyclopedia of Computer Science, 1st ed., S.v. "Data Security" by J. N. P. Hume.
- Encyclopedia of Computer Science, 1st ed., S. v. "Information Systems" by Daniel Teichroew.
- Encyclopedia of Computer Science, 1st ed., S. v. "Legal Protection of Software" by Calvin N. Mooers.
- Encyclopedia of Computer Science, 1st ed. S. v. "Security of Computer Installations. Physical" by William F. Brown and R. V. Jacobson.
- Fuori, William M; D'Arco, Anthony; and Orilia, Lawrence. Introduction to Computer Operations. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981.
- Garrett, Raymond D. Hospitals - A Systems Approach. Philadelphia: Auerbach Publishers, Inc., 1973.
- Gotlieb, C. C., and Borodin, A. Social Issues in Computing. New York: Academic Press, Inc., 1973.

- Hayes, John P. Computer Architecture and Organization. New York: McGraw-Hill Book Company, 1978.
- Hemphill, Charles F., Jr. and Hemphill, John M. Security Procedures for Computer Systems. Homewood, Ill.: Dow Jones-Irwin, Inc., 1973.
- Hodge, Melville H. Medical Information Systems. Germantown, Md.: Aspen Systems Corp., 1977.
- Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, N.J.: Prentice-Hall Inc., 1977.
- Hsiao, David K.; Kerr, Douglas S; and Madnick, Stuart E. Computer Security. New York: Academic Press, Inc., 1979.
- Huesing, Steven A. "Hospital Information Systems: An Administrative Perspective," Hospital Information Systems. Edited by Roger H. Shannon. Amsterdam: North-Holland Publishing Co., 1979.
- Kamen, Al. "Fraud Charged in Fed Computer Case." Washington Post, 5, January 1983, Sec. D, p. D1.
- Katzen, Harry, Jr. Computer Data Security. Von Nostrand Reinhold Company, 1973.
- Knapp, Thomas J. "Selling Data Security to Upper Management." Data Management, July 1983, pp. 22-25.
- Mader, Chris. Information Systems: Technology, Economics, Applications. Chicago: Science Research Associates, Inc., 1974.
- Mair, William C. "Computer Abuse in Hospitals." Hospital Progress 58 (March 1977): 61-63.
- Malvey, Mari. Simple Systems, Complex Environments. Beverly Hills: Sage Publications, Inc., 1981.
- Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, N.J.: Prentice-Hall Inc., 1973.
- Office of Technology Assessment. Computer-Based National Information Systems: Technology and Public Policy Issues. Washington, D.C.: U.S. Government Printing Office, 1981.
- Parker, Donn B. Computer Security Management. Reston, Va.: Reston Publishing Company, Inc., 1981.
- Priest, Stephen L. Managing Hospital Information Systems. Rockville, Md.: Aspen Systems Corp., 1982.

- Raymond, Samuel. "Hospital Information Systems: A Physician's Perspective," Hospital Information Systems. Amsterdam: North-Holland Publishing Co., 1979.
- Remer, Daniel. Legal Care for Your Software: A Step-by-Step Guide for Computer Software Writers. Berkeley, CA.: Nolo Press, 1982.
- Sacharow, Fredda. "Computer Criminals: A New Breed." New York Times, 4 April 1982, Sec. 21, p. 1.
- Schrage, Michael. "Computer Chips in on Crime." Washington Post, Sec. D, p. D8-D9.
- Smith, Philip. "Fairfax Man Charged with Tapping Files by Computer." Washington Post, Sec. B, p. B1.
- Sherman, Kenneth. Data Communications: A Users Guide. Reston, VA: Reston Publishing Company, Inc., 1981.
- Stern, John A., and Stern, Nancy. An Introduction to Computers and Information Processing. New York: John Wiley & Sons, 1982.
- Walker, Bruce J. and Blake, Ian F. Computer Security and Protection Structures. Stroudsburg, PA: Dowden, Hutchinson & Ross, Inc., 1977.
- Waters, Kathleen A. and Murphy, Gretchen Frederick. Systems Analysis and Computer Applications in Health Information Management. Rockville, Md.: Aspen Systems Corp., 1983.
- Wildavsky, Aaron. Forward to Simple Systems, Complex Environments, by Mari Malvey. Beverly Hills, CA: Sage Publications Inc., 1981.

VITA

Raymond Donald Wright, the son of Robert and Catherine Wright, was born on October 8, 1948, in Bucyrus, Ohio. He grew up in Upper Sandusky, Ohio, a small rural community. In June, 1966, he graduated from Upper Sandusky High School; in September of the same year, he enrolled in Stautzenberger Business College, which is located in Toledo, Ohio, and graduated in June, 1968 with a Diploma in Data Processing. While attending Stautzenberger Business College, he worked part-time as a computer operator for Toledo Business Data Services.

In July, 1968, he enlisted in the United States Air Force. For 8 years he was employed as a computer operator. In January, 1969 he began attending classes part-time at Wright State University. Later, he transferred to Parsons College and finally transferred to Park College. In July, 1975, he graduated from Park College with a Bachelor of Arts degree in Economics/Business Administration; the degree was awarded Summa Cum Laude. In October, 1976, he was commissioned a 2nd Lieutenant in the United States Air Force. He has since been employed in hospital administration. In August, 1982 he enrolled in Trinity University under the Air Force Institute of Technology sponsorship to obtain a Master's degree in computer science. On May 12, 1984, he was awarded a Master of Science degree in Computer Science from Trinity University.

Raymond D. Wright resides with his wife, Sue, daughter Latisha, and son Edward at 6026 Hopes Ferry, San Antonio, Texas.

END

FILMED

8

1944